RESEARCH ARTICLE OPEN ACCESS

One Hop and Fingerprint Techniques for Peer To Peer Multimedia Distribution

Sajna.N.S [1], Annie R Das [2]
M.Tech Student [1], Asst.Professor [2]
Department of Computer Science and Engineering
Mohandas College of Engineering & Technology. Anad
Trivandrum - Kerala

ABSTRACT
The rapid popularity of network-based multimedia applications poses many challenges for multimedia content providers to provide efficient multimedia services. Recently, there are many research interests in providing an accurate and scalable multimedia distribution service. When selling electronic content, the merchant would like each buyer to receive a same copy of the content fingerprinted with different serial number, in order to be able to trace redistributors should illegal redistribution happen. Fingerprinting strategy is used to detect illegal redistributing multimedia data by enabling the original merchant of the multimedia data to identify the original buyer of a re-issuing copy. Anonymous fingerprinting is a good solution for the distribution of multimedia contents legally with copyright protection by preserving the privacy of native buyers, whose real identities are revealed only when an illegal re-distribution occurs. However, most of the unidentified fingerprinting methods are not practical because of two main reasons: 1) the use of complex time-consuming methods and homomorphic encryption of the content, and 2) a unicast approach that does not suitable for a large number of buyers. This paper uses some previous methods of recombined fingerprints which overcomes some of the drawbacks of that paper. The recombined fingerprint technique requires a complicated graph search for finding the illegal redistributors, which needs the participation of other innocent buyers, and sincere proxies in its P2P network. This paper mainly focuses on privacy-preserving and P2P-based fingerprinting and detection mechanism.

Keywords:- Collusion Attack, Digital Fingerprint, Digital Rights Management, Secure Multimedia Distribution, Watermarking, Sip.

I. INTRODUCTION

Recently we noticed a abrupt change in network topology like Peer-to-Peer (P2P) systems. As scalability is concerned, the unicast approach in which the merchant establishes a connection with each single buyer is not a convenient strategy. However, broadcast distribution is not suitable for fingerprinting applications since different fingerprints are required for different buyers in order to guarantee traceability. The p2p network has some advantages that attract users to prefer its usage, thus by reducing the running cost very small for the merchant to distribute original content and provide end users to access data within short time. But today's P2P content distribution systems are hacked by illegal re-distributions. This activity is not only worrisome for content providers but also for the end-users of these systems. The use of copyright protection mechanisms in P2P content distribution systems poses serious privacy threats to end users, because it is being monitored for each of their activities within these systems and being held accountable for copyright infringement. Various researchers have examined the challenges characterizing these systems from diverse viewpoints, proposing strategic solutions.

Peer to peer is a type of decentralized computing system in which nodes, referred to as peers, use the Internet to communicate with each other. All the peers in this interconnected network provide resources to other peers including bandwidth, storage space, and computing power. Peer to peer systems are attractive because they do not require any particular administrative arrangements, and their decentralized and distributed nature make them scalable, bandwidth efficient and fault-tolerant.

Peer to peer applications account for

approximately 60% of Internet's traffic. Earlier research efforts in peer to peer have mainly focused on enabling large scale distributed search. But, in recent decades, a new trend is emerging where Peer to peer systems are considered as an alternative solution to enable large scale content distribution. In particular, today's peer to peer content distribution applications (Gnutella, 2000) are extremely popular among millions of users. These applications helps users to search and obtain a digital content, ranging from relatively small-sized pictures or music files, complete software packages, movies or similar types of multimedia content, in a distributed manner. Consequently large amount of data are being shared among these users on a global scale. Content distribution in peer to peer has also received attention in the research community.

The peer to peer technology for content distribution systems is beneficial to both content providers and buyers. From media companies and e-commerce vendor's point-of view, peer to peer technology enables them to make valuable content available to a huge number of peoples at low cost and better performance as compared to traditional Client-Server distribution systems. Normal Client-Server content distribution systems are dependent on a centralized server which has high cost for its initial infrastructure investment and maintenance. The lack of scalability and robustness, the server overloading and the high bandwidth requirements, are some factors that will degrade the Client-Server system performance. Compared to Client-Server distribution systems, peer to peer technology offers cost efficiency (low infrastructure cost), scalability, fault tolerance, less administrative and control requirements and exposure to a large number of users. These benefits of peer to peer are the attractive features for media companies towards adoption of peer to peer systems, e.g., Bit Torrent [Bit Torrent, 2001] is one of the most popular peer to peer distribution system used on the Internet and it create traffic on the Internet. BBC (British Broadcasting Corporation) uses Bit Torrent to distribute hundreds of episodes of various shows. Similarly, Red Hat Inc. uses Bit Torrent to distribute Red Hat Linux. Moreover, Bit Torrent has been integrated into some web browsers such as Opera and Wyzo [Wyzo-The Media Browser, 2010].

Another important concern among end users is whether the presence of copyright protection mechanism in peer to peer distribution systems can violate their privacy rules. Protecting copyright has on the privacy interests of users is significant, a tracing mechanism makes use of a record which details what multimedia files are downloaded through a specific IP address, history of files downloaded, or a list of the peers with whom a user has interacted in the past.

II. RELATED WORKS

Scheme Based on Partial Encryption [14], the secure distribution scheme proposed is investigated and improved. Since this scheme focus on distributing multimedia content by encryption and watermarking. Some new techniques determine its performance, including the security of the encryption operation, the use of the embedded watermark and check the robustness of the embedded watermark. Some drops are found in the scheme, like low encryption capacity, the data overflow due to encryption or decryption and the low correlation value caused by collusion, which reduce its performances largely. To increase the performance, some methods are introduced, including media preprocessing, media encryption based on module addition and collusion-free fingerprint encoding. Different checking exhibit that better performances are obtained by the improved methods. The analysis method proposed [14] here can be used to check some other joint fingerprinting and decryption schemes.

A new secure multimedia distribution Scheme that prevent to collusion attacks is proposed. In this scheme[15], the multimedia content is modulated by pseudo random sequences at the server side, which generates the unintelligible multimedia content, and it is demodulated with the help of the fingerprint code at the customer side, which produces the multimedia content contains an individual identification code. The demodulation process adopts collusion-free fingerprint codes to determine which sequences shall be removed from the received multimedia content. Since the collusion-free fingerprint code is used, the colluder who integrates different copies together can be detected. Compared with previous methods, the collusion-resistant code is used here gives robustness against collusion attacks. This method provides a good choice for secure multimedia data distribution.

In [16] this paper they introduce new techniques for the distribution of multimedia content in terms of media encoding and media distribution. The platform architecture includes the use of media coding techniques, including both standard and state of the research methods

like wavelets, multiple description coding techniques combined with new transport and real-time streaming protocols established over peer-to-peer networks. Invention of media resources and selection of peer nodes consider into account social networking related information and this can be used by user communities over the Internet. The design of this technique is taking place in the circumstance of the European FP7 project SARACEN.

Session Initiation Protocol [17] is an application layer signaling and control technique for creating, editing and terminating meetings containing e-phone calls, multimedia data distribution like audio, video and multimedia conferences. More flexible, extensible and open, SIP (Session Initiation Protocol) has a complete security mechanism that helps security for media and signaling. SIP RFC advice the use of TLS or DTLS to provide an extra level of protection against attacks. Moreover, avoiding from these rules is a way to perform non-repudiation service when used in SIP networks to provide a large level of trust between user agents. In this method they propose to modify and sign some header fields in the request messages in order to achieve some service over TLS/DTLS. Coming to the implementation, the success of the test of their proposal called SIP SIGN. The new messages shall be created and checked by a redirect server named as "Proxy Signatory" standing between the user agents and their local proxy servers. This server helps the caller to sign its SIP messages using certificates such as X.509 and the colleen to check and validate the signature and the caller identity.

III.SYSTEM ARCHITECTURE CONCEPT

1. System model

The participants in the proposed fingerprinting system are the following:

- Merchant: He gives the original copies of the content legally to the seed buyers. Each part of the content includes a different segment of the fingerprint. The segments have low pair-wise matching.
- Seed buyers (Bi for i = 1, . . .,M). They receive fingerprinted copies of the original contents from the merchant that are used by the peer to peer distribution system to bootstrap the system. They can be either real or substitute buyers as discussed in [10].
- Other buyers (Bi for i = M + 1, . . .,N, with M < N). They will buy the multimedia content and obtain their fingerprinted copies from the peer to peer distribution system. The content is integrated from fragments obtained from different peers. Anonymous connections with peer buyers are provided by proxies.
- Proxies. They provide unspecified communication between peer buyers.
- Transaction monitor. It produces a transaction register for each deal carried out for each buyer. The transaction register contains an encrypted version of the embedded fingerprints.
- Tracing authority. In case of illegal re-distribution happens, it includes in the tracing protocol that is used to identify the illegal re-distributor(s).

2. Security Model

The security hypothesis of the proposed system is the following:

- The merchant does not want to be trusted either for distribution or to include a pseudonym with the identity of a buyer. The rules for distribution and for traitor tracing described here are proven to work even if the merchant is not trusted.
- Buyers are not trusted and rules are provided to guarantee that 1) they are carrying authenticated fragments of the content and 2) their anonymity can be removed in case they re-distributing the original content illegally.
- The transaction monitor (or any other single party) will not have access to the clear text of the fingerprints. This prevents that any single party can blame an innocent buyer.
- Moreover privacy is concerned, the transaction monitor is not trusted then he can only access to pseudonyms, but not to the buyers real identities.
- The transaction monitor is trusted by giving symmetric keys that are used for encrypting the fragments This means that 1) the transaction monitor stores the key provided by each parent buyer and 2) this key can be used only once from its database (in principle by the child buyer). After this retrieval, the transaction monitor blocks the register and removes it.
- The transaction monitor gives the real pseudonym corresponding to an illegal re-distributor in the traitor tracing mechanism. Moreover, this trust can be changed by a group of fingerprints provided by the proxies. The tracing authority is part of a legal system and he should be trusted. It is not expected that the authority participates in any violation to frame

an trustworthy buyer or break someone's privacy.

- The interaction between the merchant and the seed buyers, and between peer buyers within the peer to peer distribution system, must be anonymous. The fragments of the content are encrypted using public cryptography.
- Proxies are not trusted and the fragments sent through these proxies shall be encrypted in such a way that only the sender and the recipient have access to their clear-text. Malicious proxies may try to cheat by sending false fingerprint segments or not reporting to the transaction monitor.
- The fingerprints are constructed with a large number of segments to guarantee that recombination will produce different fingerprints for different buyers.
- The hashing functions used in the system are more secure and cannot be inverted.
- Public-key cryptography is prohibited to the encryption of short binary strings, such as fingerprint segments or hashes. The different peers like merchant, transaction monitor, proxies and buyers have a pair of public and private keys to be used in different steps of the encryption.
- A single malicious party cannot be able to construct the fingerprinted copy corresponding to any buyer to frame a honest user of the system. In the same way, a single malicious party shall not be able to connect the identity of some buyer to a particular content unless that user is involved in an illegal redistribution of the content.

3. *Proposed Model*

In our current protocol we choose p2p network for transmitting multimedia data and anonymous fingerprinting techniques to create the fingerprint. The participants of our current protocol are sender, receiver and proxies. The intermediate nodes are known as proxies. Each peers in the p2p network having their own public and private keys. Here the original multimedia content is divided into equal sized parts. Each single part is encrypted using receiver's public key. This document is send along with fingerprint. Here we are using the public key encryption algorithm RSA. So we do not publish any type of keys for encryption and decryption.

Fingerprint is calculated by taking the checksum of the original data and divided it into equal sized fragments. Here we are doing multiple encryption using public keys of peers which are participating in the shortest path. Start the encryption using end users public key and next with second last proxy's public key.Cotinuing like that finally we will get the fingerprint. This fingerprint is appended along with the encrypted data. This whole document is sent from original owner of the multimedia data to the next intermediate node. That node uses his own private key to decrypt the fingerprint. Hence he can make the new fingerprint by removing the first cover of the incoming fingerprint. Continuing like that finally the buyer will get checksum and encrypted data. Encrypted data is decrypted using buyer's private key. He again calculates the checksum from the encrypted data. Compare this with the received checksum. In the same way he will get different packets through different paths. Check those checksums and combine the different fragments then we will get the original document or data.

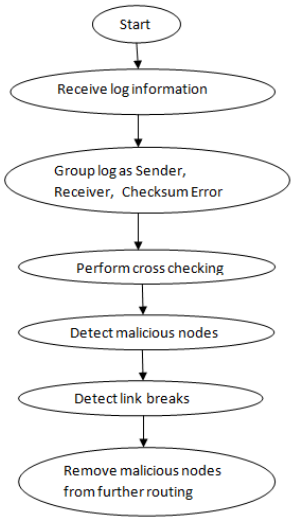


Figure1.Coordinator Setup

The coordinator acts as a server who can perform the following operations. With the help of coordinator a merchant can start the multimedia distribution process. So we first need to start the coordinator. Coordinator receive log information from the nodes those who are participating in the sending operations. The original multimedia data is divided into different fragments and each fragment is sending through different paths. The nodes those who are participating in different paths are included in the log information. He groups the log information into sender, receiver, and checksum error. Find out malicious nodes that are participating in the network and he can also remove those nodes. If number of success is lower than failure in one path and select that path as link break. Figure 1 shows the above operations.

When a merchant wants to transmit any multimedia data through a network, the nodes present in the network first create their own public and private keys. With the help of these keys encryption and decryption should perform. The different fragments in the original data are transmitted through different shortest paths. The original merchant calculate the checksum of the original data and split the whole document into different fragments. In each fragments we perform encryption and send to the next node. On receiving each fragment the nodes decrypt the checksum and send to the next node. Each node periodically sends the node information to the coordinator. The various operations a node can perform depict in figure 2.

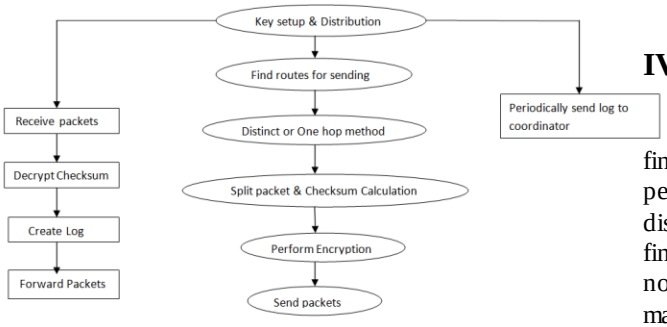


Figure 2: Node operations

The drawback of the existing system is it requires large time and inability to find out illegal re distributor. To avoid this in the proposed system we added one hop mechanism. According to this method we are adding one more hop at the end of every path. So each node doesn't know which the actual recipient is. Every node can perform two operations 1) forward the upcoming packet, 2) drop the incoming packet. If he drops the packet, sometimes the packet he redistributes is his own. So he cannot drop that. The only action he can perform is to forward the packet. But in the previous method at the time of decryption the nodes can realize that the data is not mine. So he may try to redistribute it.

One hop method removes the selfish mind of each node. According to one hop method we are adding one more node after the last node. Suppose node A wants to transmit data to node I, then this method select one more hope in the shortest path after I that is H. Where H should be minimum amount of distance from I. From H the data is transferred to the final buyer I .The network is shown in figure 3. First our protocol finds out the shortest distance using dijkstra's algorithm. .Suppose the intermediate nodes in the shortest path are B, C, F.First A encrypts the multimedia data using the public keys of nodes in the shortest path in the order of I, H, I, F, C, B .Due to this method any node never try to re-distribute the packet to some other nodes.

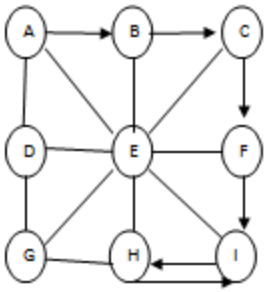
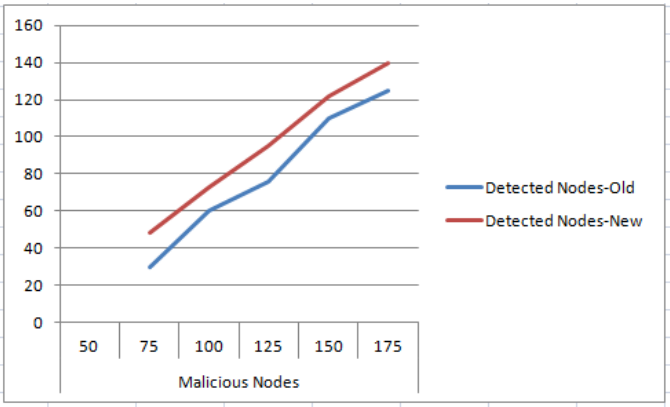


Figure 3.Data travelling through one hop method

IV.RESULT ANALYSIS

The analysis concludes that one hop and fingerprint technique for multimedia distribution out performs all other techniques relating to multimedia distribution. Here it will never distribute data once after finding malicious nodes. Server find out a malicious node in the path then it shows data transfer through this malicious node as failure. By comparing previous method and our existing system shows that it will detect more number of illegal redistributors than before.



IV. CONCLUSION

Here we use the concept of anonymous fingerprinting mechanism where honest buyers need not identify themselves to merchants, but merchants can nevertheless find out the identity of traitors who redistribute data without permission.

Fingerprinting digital contents is an attractive option to protect the rights of content authors and owners when contents are sold or distributed over the Internet.

Basically, fingerprinting consists of embedding an imperceptible mark in the distributed
content to identify the content buyer. The embedded mark is different for different buyer, but the content should be equal for all buyers. In case of illegal re-distribution happens , the embedded mark will allow identifying the illegal re-distributor.Here we use one hop method successfully to identify more number of malicious nodes.

REFERENCES

[1] D. Boneh and J. Shaw. Collusion-secure fingerprinting for digital data.
In Advances in Cryptology-CRYPTO'95, LNCS 963, Springer, pp. 452-465,1995.

[2] Birgit Pfitzmann, Matthias Schunter: *Asymmetric Fingerprinting;* Eurocrypt '96, LNCS 1070, Springer-Verlag, Berlin 1996, 84-95.

[3] M. Kuribayashi, "On the implementation of spread spectrum fingerprinting in asymmetric cryptographic protocol,"EURASIP J. Inf.
Security, vol. 2010, pp. 1:1–1:11, Jan. 2010.

[4] I. Cox, J. Kilian, F. Leighton, and T. Shamson, "Secure spread spectrum watermarking for multimedia", *IEEE Trans. Image Process.*, vol. 6, no. 5, pp. 1673.1687, 1997.

[5] T. Okamoto and S. Uchiyama, .A new public-key cryptosystem as secure as factoring,. In *Advances in Crypgology . EUROCRYPT'98*. 1998, vol. 1403 of *LNCS*,pp. 308.318,Springer-Verlag.

[6] P. Paillier, .Public-key cryptosystems based on composite degree residuosity classes,. In *Advances in Cryptology . EUROCRYPT'99*. 1999, vol. 1592 of *LNCS*,pp. 223.238,Springer-Verlag.

[7] B. Pfitzmann and M. Waidner, "Anonymous fingerprinting," in Proc.
16th Ann. Int. Conf.Theory Appl. Cryptographic Techn., 1997,pp. 88– 102.

[8] J.Camenisch,"Efficient anonymous fingerprinting with group signatures'
In Asiacrypt 2000, LNCS 1976, Springer, pp. 415-428, 2000.

[9] D. Megias and J. Domingo-Ferrer, "DNA inspired anonymous fingerprinting for efficient peer-to-peer content distribution," in Proc.IEEE Congress Evol. Comput., Jun. 2013, pp.2376–2383.

[10] D. Megias and J. Domingo-Ferrer, "Privacy-aware peer-to-peer content distribution using automatically recombined fingerprints,"Multimedia
Syst., vol. 20, pp. 105–125, 2014.

[11] S. Katzenbeisser, A. Lemma, M. Celik, M. van der Veen, and M.Maas,
"A buyer-seller watermarking protocol based on secure embedding,"
IEEE Trans. Inf. Forensics Security,vol. 3, no. 4,pp. 783–786, Dec. 2008.

[12] D. Megias," Improved Privacy-Preserving P2P Multimedia Distribution
Based on Recombined Fingerprints" IEEE transactions on dependable and secure computing, vol.12, no. 2, march/april, 2015.

[13] J. Domingo-Ferrer and D. Megias, "Distributed multicast of fingerprinted content based on a rational peer-to-peer community,"Comput. Commun., vol. 36, pp. 542–550, Mar.2013.

[14] Shiguo Lian, Xi Chen, Yuan Dong, Haila Wang,"On the Secure Multimedia Distribution Scheme Based on Partial Encryption"2010.

[15] Shiguo Lian, "Collusion-Traceable Secure Multimedia Distribution
Based on Controllable Modulation",2008.

[16] Rui Santos Cruz, , Charalampos Z. Patrikakis, Nikolaos C. Papaoulakis,"SARACEN A platform for adaptive, socially aware multimedia distribution over P2P networks",2010.

[17] Samer EL SAWDA "A trust communication with SIP protocol",2010.